DRAFT
Nebraska Information Technology Commission
Technical Panel Work Group on E-Government Architecture
E-Government Architecture Document
(Date of Last Revision: April 3, 2001)

A. Authority

Section 86-1506 (6). "(The Nebraska Information Technology Commission shall) adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel created in Section 86-1511."

Section 86-1510 (2). "(The Chief Information Officer shall) recommend policies and guidelines for acceptable and cost-effective use of information technology in non-education state government."

Section 86-1511 (2). "The technical panel may recommend technical standards and guidelines to be considered for adoption by the commission."

B. Purpose and Objectives

The Statewide Technology Plan establishes a state enterprise architecture framework to provide guidance on various aspects of the state's technical environment. Electronic government architecture is one component, which is necessary to support deployment of e-government information and services.

E-government, e-business, and e-commerce represent the introduction of a recent wave of technological innovations. For purposes of this document, e-government is defined as "the use of technology to enhance information sharing, service delivery, constituency and client participation, and governance by transforming internal and external relationships." This includes transactions between government and business, government and citizen, government and employee, and among different units and levels of government.

The Technical Panel of the NITC chartered a work group to make recommendations on what components make up an efficient and robust foundation to support e-government. This document sets forth some basic principles, guidelines and standards towards this end. The e-government architecture must be consistent with the state's technical infrastructure.

The fundamental purpose of the e-government architecture is to facilitate implementation of citizen-centric access to information and services and support deployment of other e-government applications. The architecture can reduce the time and cost of deploying applications, while making it easier to integrate information and services.

The following principles should guide the development of the state's e-government architecture:

1. The architecture must promote integrated access and delivery of information and services in a manner that is convenient and easy to use.
2. The e-government architecture must support the mission of the agency;
3. The e-government architecture must facilitate business transformation to improve customer service, achieve cost savings, and reduce complexity.

4. The e-government architecture must promote enterprise requirements including security and privacy, aggregation of demand, efficiencies, collaboration within communities of interest, ease of use, and integration of services;
5. The e-government architecture must provide adaptability to accommodate change and permit fast deployment of e-government solutions;
6. The architecture must encourage creativity, initiative, and innovation by agencies;
7. The e-government architecture must accommodate change in technology and changing requirements.

C. E-Government Architecture

POLICY STATEMENT

The e-government architecture consists of three conceptual layers:

- Presentation
- Enterprise Services
- Applications and Data

The presentation layer starts with the state's gateway for access to electronic records, pursuant to the Records Management Act (Chapter 84, Article 12). It includes any interface between the user and e-government information and services. Enterprise services are the support systems that are necessary for delivering applications and information to users. The applications and data layer provide the specific information or resources sought and valued by the user.

The e-government architecture must support the principles and objectives listed in the previous section. The architecture should be viewed as a process for arriving at decisions rather than a static set of standards and guidelines regarding the infrastructure for e-government services. Architectural planning should strive to "engineer out" inhibitors to change, "engineer in" ways to maximize the effectiveness of information technology, and take care to minimize risk.

GUIDELINES

1. Presentation Layer.
   Definition: The presentation layer provides the means for the user to access and interact with the application and data.

   Goals and objectives:
   a. Support integration of information and services across agencies, institutions and jurisdictions;
   b. Allow features, which make it easier for the user to obtain information and services targeted to specific areas of interest;
   c. Permit effective searches of information and services;
   d. Follow basic design principles that promote ease of customer use and compliance with critical requirements, including security, privacy, and accessibility. Design principles shall preserve opportunities for creativity and allow customization for target audiences.
   e. Provide easy access to help, including FAQs, technical assistance, and means of contacting subject matter experts and persons in authority;
   f. Meet state and federal standards for accessibility.

Description:
The Records Management Act (Sections 84-1201 through 84-1228) recognized the need for a "centralized electronic information system" for accessing public records. The State Records Board has the authority to designate a "network manager" to operate the state's electronic "gateway" to information and services. As the state's electronic "gateway", Nebraska Online has the responsibility of exploring ways and means of improving citizen and business access to public records and services.

Although Nebraska Online provides centralized access to state government information and services, individual agencies maintain their own web sites. These web sites range from very basic in terms of content and organization to extensive. Each site represents part of the presentation layer. Nebraska Online and individual agencies are constantly adding content and improving functionality, including interactive services.

The mix of centralized and decentralized responsibility for the presentation layer presents several advantages and challenges in terms of meeting the goals listed above. Advantages include greater innovation and responsiveness to the needs of agencies, while still providing a single point of access through the network manager. Challenges include providing the user with a consistently intuitive, high quality experience coupled with seamless access to information and services.

Although they do not receive as much attention as the Internet, other technologies are also part of the presentation layer. These include voice response units and kiosks.

Statements of Direction:

a. The current combination of centralized and decentralized responsibility for the presentation layer will continue for the foreseeable future.
b. Ease of use across web sites requires some standardization of navigation methods, layout and common links. All web sites should also conform to privacy policies and accessibility requirements. Web sites should be designed within technical constraints presented by the user's environment. These include the need for browser compatibility and the accommodation of multiple network connection speeds. An interagency task force of web masters should develop style guidelines to address these issues, while preserving as much as possible the advantages of innovation and creativity.
c. The growth of information and services requires a central search and indexing function that is robust and scalable. The search and indexing function must be capable of yielding meaningful results that are directly relevant to the intended topic. The search function must be easy to use and permit progressive choices that narrow the search results. The domain of the search should be user-specifiable and range from a single agency through a collection of functionally related agencies. As manager of the central electronic gateway, Nebraska Online should evaluate different options for improving the search and indexing function for state government web sites. If necessary, agencies should add tags and other information that would enhance the search function.

d. The presentation layer should make it easy for customers to find help. This should include a visible tab on all pages. "Help" includes general access information and context-specific information. There should be a customer service search engine for frequently asked questions (FAQs) as well as access to the name, phone number, and e-mail of the individual(s) who can address their specific issues.

2. Enterprise Layer.

Enterprise services are the support systems that are necessary for delivering applications and information to users.

The Enterprise Layer should meet the following goals:

- Provide services that are most economically centralized, provided commonly, or guided by common standards for all agencies and users.
- Facilitate fast deployment of applications by providing underlying services to agencies.
- Promote citizen-centric access.

The Enterprise Layer includes, but is not limited to the following major components.

- Accessibility
- Availability
- Digital Archiving
- Encryption
- Help Desk for State Web Site and Software Developers
- Help Desk for Users
- Integration Services
- Network and Virtual Private Networks
- Payments
- Privacy
- Search Engine Tools
- Secure Signatures
- Security
- Shopping Carts

a. Accessibility

Definition: Accessibility means easily approached and obtained. In the context of e-government architecture, it refers to the ability of persons with visual and other disabilities to be able to use the information technology systems that public agencies and institutions develop for delivering information and services. Accessibility also refers to whether the information technology system reaches certain groups of users. This problem is sometimes called the digital divide.

Goals and Objectives

i. E-government applications will meet the accessibility requirements of users with physical disabilities.

Description

Several activities are underway relating to accessibility for persons with physical disabilities. The federal government recently adopted rules and

regulations pertaining to Section 508 requirements for information technology. The Technical Panel of the NITC established a work group to prepare standards and guidelines, with a checklist to assist implementation. The Assistive Technology Project, located in the Nebraska Department of Education provides advice to agencies and educational institutions on how to comply with accessibility requirements. Their web site (http://www.nde.state.ne.us/ATP/TECHome.html) is a source of information.

The Community Council of the NITC is developing several strategies that address the digital divide. The Community Council sponsored development of a database of sites where the public can use computers and access the Internet. The web site for the database is: http://www.nitc.state.ne.us/itc/community/pubaccess.htm.

Statements of Direction

i. E-government systems shall adhere to standards and guidelines for accessibility adopted by the NITC (currently under development by the Technical Panel of the NITC).
ii. Acquisition of applications and systems shall adhere to the Technology Access Clause developed by the Technical Panel of the NITC.
iii. Systems for providing information and services to the general public should consider multiple delivery methods, including the Internet, automatic voice response units, as well as traditional means.

b. Authentication

Definition: Authentication is the process for verifying the identity of an individual and limiting the individual's access to prescribed information and transactions.

Goals and Objectives

i. Prevent unauthorized access to sensitive information and critical systems.
ii. Make it as easy as possible for authorized users to access information and systems as required
iii. Integrate authorization to facility single sign-on for access to multiple systems and/or databases.

Description

Nebraska Online (NOL) provides authentication for premium services that require payment of fees as well as authentication for agency staff to update websites hosted by NOL. From time to time other non-premium services (free to the user) may require authentication. The authentication process includes assignment and administration of usernames and passwords. IMServices is deploying LDAP capabilities. Different agencies use a variety of other means for authentication.

Authentication serves as a method to challenge and validate a user at the perimeter of the State's network. Several validations can be accomplished at the point where the challenge occurs. Currently, IMServices is looking at an authentication scheme that utilizes a

Lightweight Directory Access Protocol (LDAP) schema. The LDAP Server will provide the potential for a standard interagency directory that utilizes replications to a centralized directory server (the LDAP server).

At the point of entry to the State's network, the user is asked for a username and password. When the user enters the username and password, their credentials are checked against the LDAP server to see if they are authorized to enter the requested area. If the user is authorized to enter, they are permitted access otherwise they are redirected to another area.

The advantage of an LDAP server is the distributed management of the individual agency services to a client and then replicated to a centralized LDAP server. With the standard schema in place at the State, replication and a single point of entry can better be achieved. The LDAP servers can therefore be utilized as a method of providing information to authenticate users.

Eventually, it may be possible to offer single sign-on for users, which would provide greater convenience in some circumstances. Decisions about authentication must balance the goal of ease of use against other considerations, including the feasibility of integrating applications, the difficulty of registering with the authentication authority, and the additional security provided by multiple authentication steps.

Statement of Direction

i. Authentication should be used only when security requires additional measures for protecting privacy, preventing improper access to sensitive information or critical systems, or when necessary to provide voluntary personalization of the user's experience.
ii. The choice of authentication methods should correspond to the security requirements of the specific application and data.
iii. IMServices should continue developing LDAP technology for agencies that require a high degree of security.
iv. NOL and IMServices should take the lead, involving others as needed, to develop single sign-on for authorization to multiple systems and databases.
v. Authentication processes should implement the State's security policies.

c. Availability

Definition: Availability refers to the ability of a system to be operational when required.

Goals and Objectives

i. Provide access 24 hours per day, 7 days per week.
ii. Minimize periods of unavailability, whether planned or unplanned;
iii. Provide equipment, personnel, and procedures to restore systems availability, when problems arise.

Description

Availability includes the concepts of reliability, back-up and recovery, planned maintenance, and adequate response time. The Technical Panel of the NITC recently developed a Disaster Recovery Policy as part of the comprehensive set of security policies. The purpose of the Disaster Recovery Policy is to insure continuity of government operations and to protect the safety and integrity of public records. The policy calls for owners of information technology systems to prepare risk assessments and contingency plans for business resumption. Availability also entails protection against denial of service attacks or repetitive access that impedes access by other users.

Statement of Direction

i. E-government systems shall adhere to the NITC's policy on disaster recovery. A copy of the policy is located at: http://www.nitc.state.ne.us/tp/workgroups/security/policies/sections_for_graph/sectionBandCfor_3.pdf.
ii. The Technical Panel should sponsor the development of templates and examples to assist agencies with conducting risk assessments, classifying systems, and developing contingency plans for disaster recovery.
iii. Agencies should consider opportunities for collaboration to reduce the cost of achieving high availability requirements for e-government applications.

d. Digital Archive

Definition: A facility for the long-term retention of data in electronic format.

Goals and Objectives:

i. Develop and implement standards for identifying data, which is appropriate for or requires long term retention;
ii. Provide for long term storage and retrieval of data in electronic format regardless of format;
iii. Provide sufficient security to ensure that the data stored will not be damaged, tampered with, or altered.

Description

The volume of data records created and stored by government entities solely in electronic format or converted from paper to electronic format has increased, and with it the need to provide for long term retention strategy for such records. Government records such as databases, e-mail, and web sites, may have long term retention value and exist only in electronic form. Currently the state has no standards for the long retention of data in electronic format.

Issues that will need to be addressed in order to implement a strategy for a digital archive include the following. Developing record retention schedules specific to electronic data such as e-mail. Developing and providing a classification system to sort and send electronic records to the proper retention site. Developing a long-term storage facility, which will address such issues as software version changes, degradation of media

over time, physical security of data, and availability of hardware capable of reading archived data.

The Secretary of State's Office, Records Management Division, is currently working with IMServices to develop a pilot digital archive service which could provide the services described above in the future.

Statement of Direction

i. Continued work and development of the SOS-Record's Management Division pilot project for long term digital records retention.
ii. Development of a funding model and cost estimates for a centrally administered digital archive service.

e. Encryption

Definition: Encryption is the technical process of securing data transmitted over communications media from unauthorized access.

Goals and Objectives:

i. Define what classes of data (personal information, credit card numbers, etc.) collected or transmitted by government agencies should be encrypted, and at what level;
ii. Implement the most appropriate and cost-effective technical approaches to meet encryption requirements determined in #1;
iii. Stay current with changes and new developments in the area of encryption.

Description

With the explosion of data transmission over public communications networks such as the Internet, security risks emerge. In many cases, these risks are slight to non-existent because the data transmitted is not compromised if viewed by someone other than the intended audience. However, many e-Government applications – particularly those involving transmission of such things as personal information or credit card numbers – require protection from unauthorized access.

The most common solution to this security risk is encryption, a technical process by which data is transmitted in a form that can only be viewed by the intended audience. As with other security measures, encryption can be approached in degrees, from highly-secure measures that virtually no one can decrypt to less stringent encryption that could be compromised by skilled technicians. And, as with other security measures, the degree of encryption required is dependent on the degree of sensitivity of the data, and there is a relationship between degree and cost.

The fundamental premise of encryption is the same in the technical environment as it was prior to the advent of computers: the sender and receiver must agree on the encryption code that allows both the encrypting and decrypting of the data. This is commonly accomplished with a set of digital keys, usually paired as a “public key” (freely available to anyone) and a “private key” (securely stored on the user’s hard drive).

There are a number of companies in the market today that provide public key cryptography, but their use is not presently widespread.

Secure Sockets Layer (SSL) is a protocol that employs private key encryption to allow data entered through a web site to be encrypted before transmission. This is commonly used for e-commerce and e-Government applications requiring transmission of credit card information. An encrypted SSL connection requires all information sent between a client and a server to be encrypted by the sending software and decrypted by the receiving software, thus providing a high degree of confidentiality.

Statement of Direction

i. Data transmission among government agencies, citizens and businesses should include a level of encryption appropriate for the data class(es) being transmitted;
ii. Certain types of information collected by government agencies from citizens and businesses (such as credit card numbers) should be encrypted by the most appropriate means, currently SSL.

f. Help Desk for State Web Site and Software Developers

Definition
Goals and Objectives
Description
Statement of Direction

g. Help Desk for Users

Definition: As used here, "Help Desk" refers to the full range of methods for providing technical assistance to the end customer when using the tools of e-government.

Goals and Objectives

i. Provide easy access to technical assistance for end users;
ii. Encourage self-service by users;
iii. Save time and effort for agencies when deploying e-government
iv. Provide an easy means to contact subject matter experts and persons in authority;
v. Improve the content and robustness of the help desk through collaborative efforts.

Description

E-government strives to be user-friendly with trouble-free access to information and services. The complexity of technology and the broad range of abilities on the part of users makes this is an impossible goal. The purpose of a help desk is to plug the gap between the ideal and the reality. Examples of help desk functions include explaining how to navigate through the web sites, how to use the search function or how to download and use Adobe Acrobat. Finding the right person to lodge a complaint or report technical problems are other examples.

Statement of Direction

i. Develop a central repository of FAQs and assistance for common problems;
ii. Use automated tutorials and other interactive methods, where feasible;
iii. Providers of e-government systems will track user questions and problems in order to build on experience and address areas of weakness.

h. Integration services

Definition: Integration services refer to applications and tools that facilitate the exchange of data between otherwise incompatible systems.

Goals and Objectives

i. Document current methods in use that serve this purpose;
ii. Identify best practices and recommend other methods;
iii. Develop skill sets to make effective use of integration services.

Description

E-government promises to reduce jurisdictional barriers by offering integration of information and services. One approach to achieving integration is one-to-one interfaces and data exchanges. Another approach is to use integration services such as "middleware", message brokers, or other tools for automating the exchange of data, without requiring a customized interface for each pair of applications. One example of the need for integration methods is with data for geographic information systems (GIS). GIS makes it possible to combine a wide range of data and maps to produce new information and analyses. Combining these disparate data types from multiple independent entities requires some agreement on format or methodologies.

Statement of Direction

i. Monitor changes in technology, future opportunities and developments;
ii. Recommend topics for further evaluation.

i. **Networks and Virtual Private Networks**

Definition: A network is comprised of communications media (wired or wireless) and the electronics required for communicating voice or data from one place to another. A Virtual Private Network provides a dedicated, secure path to improve performance and reliability.

Goals & Objectives:

i. All agencies should have direct access to the state core network. Decisions need to be made regarding the cost of access and source of funding.
ii. All units of state & local government should have direct access to a TCP/IP network to facilitate eGovernment.

Description:

For eGovernment applications, the Internet (sometimes referred to as a "network of networks") provides the vast majority of government-to-citizen

and government-to-business network access. However, networks internal to government must be adequate to move information from place to place in support of eGovernment applications.

The state has a robust core network that currently provides the internal network support necessary for eGovernment applications. However, not all agencies are currently connected to this core network. This causes impediments that hinder eGovernment efforts. For example, online renewal of electrician licenses has not worked as effectively as it could due to network limitations.

Nebrask@ Online currently provides, at no cost, dial-up connections for some agencies not connected to the core network, including the Nebraska Historical Society and State Auditor. This consumes NOL's local modem pools, resulting in less-than-adequate services not only for the agencies, but also for local dial-up customers outside of government.

Resolution is being evaluated and implemented to provide network access to all agencies that are currently being serviced by dial-up services. Therefore eliminating the reduced bandwidth to the agencies utilizing dial-up services.

Virtual Private Networks (VPN's) are also being implemented to reduce the cost by moving the point of entry into the State's network to the local Internet Service Provider of the client or employee. The VPN can then be used to access the State's network via local dial-up's, ADSL, or Cable Modem Service in the local service area of the customer or employee. The VPN service is available today and is being utilized by customers to access the address-translated portion of the State's network.

Statement of Direction:

i. Resolution must be achieved regarding issues preventing all agencies from having direct access to the state core network.
ii. Efforts should continue to bring local governments, and remote locations for state agencies, onto a direct TCP/IP network connection.

j. Payments (Payment Processing)

Definition: Payments or payment processing refers to the electronic collection of fees for services such as licenses, permits, registrations, or data access.

Goals and Objectives:

i. Provide the capability for users of online government services to pay any necessary fees electronically via credit card, electronic check, or other viable means.
ii. Ensure that each electronic payment processing method provides effective security to prevent fraudulent acquisition and use of credit card, checking account, or other payment information.

Description:

Electronic payment processing via credit card has existed for several years, and adoption by users is increasing. Online retailers throughout the world offer secure credit card payment options for just about anything that can be purchased online. In Nebraska, the Game & Parks Commission and the Health & Human Services System have accepted credit cards via the web for some time, with no apparent compromise in security of payment information. Benefits of electronic payment processing include convenience for the user, and faster collection of revenue for the agency.

A more recent electronic payment method is the electronic check, or customer-initiated ACH transaction. It works very much like a credit card payment process, but instead of entering credit card information the user enters a checking account and bank routing number. This method is beginning to emerge as an alternative to credit card payments, and provides a benefit to agencies that must pay charges to banks and processing agents.

Unlike credit card transactions, where the charges are based on a percentage of the payment amount, electronic check charges are typically a flat fee regardless of the payment amount. Discussions are under way between Nebrask@ Online and the State Treasurer to pursue this option for Nebraska agencies.

Statement of Direction:

i. As more government services move online, agencies should incorporate electronic payment processing as the preferred means of collection for any fee associated with the service.
ii. Security of payment information, including credit card or checking account numbers, cannot be compromised. Encryption and other suitable methods of securing the information must be utilized effectively and constantly.

k. Privacy

Definition: Privacy means keeping information confidential, if it is not a public record and available for public use.

Goals and Objectives

i. Improve and maintain the public's trust in government regarding protection of privacy.
ii. Protect the confidentiality of information, if it is not a public record.

Description

All information which is collected by state agencies is likely to be considered a public record which is available for public review under the Nebraska Public Records Statutes unless there is a specific statute which allows that information to be kept confidential. An example of a specific statute, which allows certain types of information to be kept confidential, may be found at Neb. Rev. Stat. Section 84-712.05.

The State's e-government strategy calls for making an increasing amount of information available to the public on the Internet. Even if not

published on the Internet, more agencies are storing a growing amount of information on computers. Digital format and easy accessibility of information make it possible to aggregate and manipulate large amounts of data. It is also possible to create new information by linking data from multiple records on the same individual. For example, one analysis claims that 87% of the time, someone's birth date, gender, and five-digit zip code are sufficient to establish a unique record, which can then be combined with information from other sources.

Trust is an important issue. According to one national survey (Hart-Teeter, September 2000), 65% of the public wants government to proceed slowly with implementing e-government, because of concerns about security, privacy, and access. Fifty-three percent of the public is very concerned about e-government resulting in less personal privacy. According to another national survey, (Civic.com, April 2000, page 22) 85% of respondents "regarded the privacy of information transmitted online as the most important issue the Internet faces."

Privacy policies should recognize the ability to share confidential information with qualified agencies or partners.

Statement of Direction

i. State agencies and institutions must develop and implement privacy policies and procedures to protect confidential information, which is not a public record. Privacy policies should provide guidance on sanitizing records so that public records can be released without compromising confidential information.
ii. E-government applications must implement privacy and security methods that will protect confidential information.
iii. Agencies and institutions should avoid collecting personal information that is not essential to the service being provided.
iv. For credit card transactions, agencies and institutions should retain the authorization code rather than the credit card number.
v. Agencies and institutions should collaborate on implementing technologies that protect privacy, such as encryption, secure signatures, LDAP directories, and security measures.
vi. The state's portal should include a web site with links to all statutes pertaining to public records.
vii. Before making information available on the Internet, agencies should revise their record retention policies to insure compliance with the Records Management Act and other statutes pertaining to public records.

l. Search Engines & Tools

Definition: A search engine is a tool for finding information on the world wide web via key words or other criteria. Sometimes referred to as “spiders” or “crawlers,” search engines typically display results in groups of 10 to 100 and provide direct links to the sites found during the search.

Goals & Objectives:

i. Search engines for government information and services should retrieve information about or contained in agency web sites in the most consistent, thorough and relevant manner possible.
ii. Agencies should use appropriate metatags or other techniques to allow government search engines to function in the most effective manner possible.
iii. Other search tools, including site maps, category-based menus, and direct contacts to information professionals such as librarians should be used to supplement online search engines as a means of effectively finding information.

Description:

The good news about the information age is that an unprecedented volume of information and services are available on the web. The bad news is that finding what you are looking has become a substantial challenge.

Search engines are one way to sort through the vast amounts of information in order to find resources most relevant to the user's needs. The effectiveness of search engines is increasing, and there are several large engines available to search the entire contents of the web.

Nebrask@ Online has developed a search engine accessible from the state portal for information and services specific to state government. The engine operates via an index of all agency sites with the "state.ne.us" suffix, as well as alias URLs (such as "treasurer.org") that point to state government sites. The engine can be easily customized for use by specific agencies. Some individual agencies have other search engines located on their home pages.

NOL also uses other search tools on the portal, including a detailed, citizen-centric list of information categories, a site map, and a direct link to the Nebraska Library Commission's "Ask a Librarian" site. The latter includes additional search tools as well as contact information to put the user directly in touch with a reference librarian.

Statement of Direction:

i. Agencies and Nebrask@ Online should collaborate in an effort to continuously upgrade the reliability and effectiveness of search engines & tools used to guide citizens toward the information and services they seek.
ii. Consideration should be given to using metatags or other means to improve the precision of searches.

m. Secure signatures

Definition: A secure signature provides a means by which documents and filings can be authenticated, validated, approved or endorsed electronically.

Goals and Objectives

i. Provide a method by which externally and internally generated documents may be signed and endorsed electronically.
ii. Ensure that the convenience and security of using an electronic signature meet or exceed the standards for manual signatures.

Description

Secure authentication of documents is a key tool in implementing an e-government strategy. At this time there is no single standard or technology that has emerged for creating secure signatures electronically. Public key encryption is one technology that provides a means to endorse documents and also encrypts the endorsed document to minimize the possibility of altering or tampering with the signed document. However, there are still issues of compatibility across vendors, cost, and public understanding and acceptance of this technology for widespread use.

The State of Nebraska recognizes secure signatures generally through the Uniform Electronic Transactions Act (UETA) and specifically through the Digital Signatures Act. UETA generally states that transactions shall not be invalid solely because they are in electronic form, but does not give any specific guidelines for digital authentication. The Digital Signatures Act specifically recognizes public key encryption and signature dynamics (an electronic record of a manual signature) for all transactions requiring a signature, and recognizes pin numbers and passwords for transactions with government entities as long as certain criteria are met.

The pin number and password approach may be appropriate for certain license renewals or annual fee payments, but some issues still exist where a greater degree of security is needed. One example is when the individual is undertaking the first transaction with the state and no electronic signature or identifier has been assigned. Another example is when notarization is required.

Statement of Direction:

i. Develop a strategy for a single electronic signature, which could be used by an individual or entity doing business with any agency.
ii. Consider statutory changes to allow for digital notaries or change or eliminate notarial requirements in certain instances.
iii. Monitor national and international developments in this area to see what standards emerge either by law or custom and practice;
iv. Prepare best practices that agencies can use to address common problems.

n. Security

Definition: Information Security is the protection of data against accidental or malicious destruction, modification or disclosure.

Goals and Objectives

i. Insure continuity of government operations.
ii. Protect the safety and integrity of public records.
iii. Prevent unauthorized access to public records.

Description

The NITC has adopted a comprehensive set of security policies (January 23, 2001). The Technical Panel of the NITC has identified security as a priority issue and continues to work on ways to assist agencies with implementing security issues.

The security policies recognize that security is an on-going activity, which requires decisions that affect the level of protection of data and systems. This requires continual assessment of risk and adoption of security measures that are commensurate to the security needs of the information and computer resources.

Security is a shared responsibility because of interconnected networks and Internet access. Agencies and institutions must implement e-government applications in a manner that prevents unauthorized access or use, maintains availability and protects the security of information resources. Agencies and institutions must establish controls that are commensurate to the security needs of the information and computer resources on the network. Controls shall also reflect the security needs of other agencies or institutions connected to the network.

Statement of Direction

i. E-government systems shall adhere to the NITC's security policies.
ii. The Technical Panel should sponsor the development of templates, examples, and training to assist agencies with implementing security policies.
iii. Agencies should consider opportunities for collaboration to reduce the cost of implementing security requirements for e-government applications.

o. Shopping carts

Definition: A shopping cart is a software package that allows a user to select any number of items from an online catalog or menu and place a single order or make one payment for multiple items, through a web browser.

Goals & Objectives

Optimize the speed with which shopping cart capability can be reliably integrated into eGovernment applications such as license renewals and product ordering.

Description

Shopping cart technology enables the transformation of a web site into a transactional tool that integrates online catalogs with ordering, payment and sometimes fulfillment. Shopping carts have been used for several years by online retailers, and are now coming into frequent use with eGovernment applications.

The web presentation layer is normally a “store front” that provides navigation for the user through the various transaction options available on the site. Users are able to select options (such as which licenses or permits to renew) and add them to the shopping cart. Once the user has

completed his or her selections, the shopping cart assembles them into a "check out" screen. Amounts due are totaled, and the option of credit card or electronic check payment can be provided. The system then takes the user into an encrypted section of the web site to enter payment information.

There are many commercially available shopping cart packages supporting a variety of programming languages. However, in most eGovernment applications, integration with a back-end system (database) is required so custom development is necessary. Variations in agency business rules may also increase the complexity of implementing shopping carts. For example, some agencies have different fees for the same license or registration based on a particular user's volume.

Statement of Direction

Move toward the most cost-effective solution(s) for rapid deployment of shopping cart technology to support eGovernment applications. Both commercial and open source shopping cart software should be evaluated in terms of cost (licensing & support), scalability, and ease of integration into back-end systems.

3. Applications and Data.

IMPLEMENTATION

Policies and standards for the e-government architecture are intended to save time, reduce costs, and improve delivery of information and services across jurisdictional boundaries. Policies and standards are also essential for assuring certain enterprise requirements, such as privacy and security. To be successful, implementation of a standards-based architecture must include the following components:

- The standard-setting process must be open, transparent, and grounded on the principles in Section B. Affected entities must have the opportunities to propose standards, participate in developing standards, and suggest changes. All standards should be justified based on one or more of the principles in Section B. The process must insure responsiveness. The process must not lock in old technologies or slow the deployment of new technology that positions the state to achieve the principles in Section B.
- To the greatest extent possible, policies and standards should encourage voluntary compliance. People should adhere to the architecture, because it is the best way to do business. Incentives may include separate funding for enterprise projects, lower costs, faster deployment, best practices, ease of collaboration and integration, and other benefits of a standards-based architecture.
- Mandatory requirements must clearly indicate the justification in terms of adverse effects on other entities and the principles in Section B.
- Any mandatory requirement must include a process for exceptions and appeals. Exceptions should address ways to mitigate any adverse

impact. The appeal process should allow for review and determination by an independent third party.

- Implementation should follow a migration plan for an orderly transition, which allows sufficient time in order to protect existing investments in information technology.

a. Topic A (To be defined)
Definition
Goals and Objectives
Description
Statement of Direction

b. Topic B (To be defined)
Definition
Goals and Objectives
Description
Statement of Direction

D. Key Definitions

1. Agency shall mean any governmental entity, including state government, local government, or third party entities under contract to the agency.
2. Authentication - process of verifying the identity of the sender and the integrity of the message. This can be done through the use of SSL, PKI, or other mechanisms.
3. Digital Certificate – a record that is used to establish a secure connection. It contains information about who it belongs to, who it was issued by, a unique serial number or other unique identification, valid dates, and an encrypted "fingerprint" that can be used to verify the contents of the certificate.
4. E-Business -- is any process that a business organization conducts over a computer-mediated network. Business organizations include any for-profit, governmental, or nonprofit entity. Their processes include production, customer, and internal or management-focused business processes.
5. E-Commerce -- is any transaction completed over a computer-mediated network that involves the transfer of ownership or rights to use goods or services.
6. E-Government -- is the use of technology to enhance information sharing, service delivery, constituency and client participation, and governance by transforming internal and external relationships. E-business and e-commerce are subsets of e-government.
7. Electronic Signature – an electronic record usually attached to a larger record that is used by an individual as the legal equivalent of a handwritten signature.
8. LDAP --
9. PKI (Public Key Infrastructure) – a system for issuing and validating digital certificates, including a root certificate authority a certificate repository or directory, a certificate practice statement and trained individuals performing trusted roles to operate and maintain the system.
10. SSL (Secure Sockets Layer) – a protocol designed by Netscape Communications to enable encrypted, authenticated communications across

the Internet. Users on both sides are able to authenticate data and ensure message integrity.

E. Applicability

GENERAL STATEMENT

These policies are intended to be sufficiently generic to apply to a wide range of governmental and educational agencies in the State of Nebraska. Compliance with these policies and standards will be a requirement during consideration of funding for any projects requiring review by the NITC.

EXCEPTION STATEMENT

The principles in Section B provide the basis for determining the applicability of these policies and standards to specific situations within an organization. The responsible authority within an organization should establish a test for determining whether to allow exceptions to these policies and standards. The test should be based on the principles in Section B, in particular:

1. Serving the agency's mission can best be accomplished by allowing an exception;
2. An exception is necessary to promote innovation, accommodate change or allow fast deployment of e-government solutions; or
3. An agency can demonstrate that the benefits from allowing an exception outweigh the benefits of adhering to the particular policy or standard.

COMPLIANCE AND ENFORCEMENT STATEMENT

The governing board or chief administrative officer of each organization must develop internal compliance and enforcement policies as part of its information management program. The NITC intends to incorporate adherence to e-government architecture policies and standards as part of its evaluation and prioritization of funding requests.

E. Responsibility (to be defined)

Effective e-government architecture involves cooperation of many different entities. Major participants and their responsibilities include:

1. Agencies and Institutions.
2. Chief Information Officer.
3. Communications Division
4. Enterprise services providers.
5. Information Management Services Division (IMServices)
6. Nebraska Information Technology Commission. The NITC provides strategic direction for state agencies and educational institutions in the area of information technology. The NITC also has statutory responsibility to adopt minimum technical standards and guidelines for acceptable and cost-effective use of information technology. Implicit in these requirements is the responsibility to promote adequate e-government architecture through adoption of policies, standards, and guidelines. The NITC must develop strategies for implementing and evaluating the effectiveness of the state's e-government architecture.
7. Network Manager for Nebraska Online. Pursuant to Section 84-1205, the network manager shall direct and supervise the day-to-day operations and

expansion of a gateway or electronic network to make public records available electronically. The Network Manager shall recommend standards and guidelines to the Technical Panel that would promote the goals of the presentation layer of the e-government architecture.

8. State Government Council.
9. State Records Board. Pursuant to Section 84-1204, the State Records Board provides oversight of the network manager, approves reasonable fees for electronic access to public records, and improves citizen and business access to public records and services of the electronic gateway.
10. Technical Panel E-Government Architecture Work Group. The NITC Technical Panel, with advice from the E-Government Architecture Work Group, has responsibility for recommending policies and guidelines and making available best practices to operational entities.
11. Other roles and responsibilities.

F. Related Policies Standards and Guidelines

This document provides the general policies and future directions for those components that make up an efficient and robust foundation to support e-government. Related policies, standards and guidelines include:

1. Security Policies
2. Privacy Policies
3. Accessibility Standards
4. Style Guidelines